Remarks

The present amendment is made in response to the first Office Action dated June 10, 2002. In the Action, the Examiner has objected to noted portions of the specification and claims 11, 21, and 31, has rejected claims 1-7 and 16-20 under 35 U.S.C. 112, second paragraph, rejected claims 1-3, 5-12, 14-18, 21, and 29-32 under 35 U.S.C. 102(e) as anticipated by U.S. Patent 6,315,195 to Ramachandran, rejected claims 4 and 21-28 under 35 U.S.C. 103(a) over the combination of the '195 patent and U.S. Patent 5,712,912 to Tomko, rejected claim 13 also under 35 U.S.C. 103(a) over the '195 patent and U.S. Patent 4,768,021 to Ferraro, and also rejected claims 19 and 20 under 35 U.S.C. 103(a) over the '195 patent and U.S. Patent 6,129,273 to Shah. By way of this amendment, original claims 1-32 are cancelled and replaced by added claims 33-54. A check in the amount of $55.00 and Petition for One Month Extension of Time are submitted herewith. If any other changes or additions are necessary authorization is hereby given to charge our Deposit Account No. 50-0576. Claims 33-54 remain pending in the present application.

The one prior art reference relied upon in making all prior art based rejections in the Action is the '195 patent to Ramachandran. Ramachandran teaches a "smart" credit card that comprises a single electronic device having a biometric security enabling device, a magnetic stripe reader and memory for reading and storing data off of traditional credit/debit cards, including PIN data associated with each credit/debit card, manual indicia entry keys for visually associating each credit/debit card with a particular memory storage location, a visual display for permitting the user to see his/her selection of a particular credit/debit card, and a remote communications port,

such as a modem. Thus, the Ramachandran device permits its users to use a single electronic card to serve as the role of multiple individual, traditional credit/debit cards.

The fundamental difference between the present invention and that taught by Ramachandran is that the present invention bears absolutely no relationship to any other device held by its users. The function of the present invention is to securely generate, store, and manage what are generically referred to as passwords, which could be a passcode, a PIN, or the like. The passwords are generated, i.e., created, by the device, not input into the device from a separate source, as with Ramachandran.

It would frustrate the purpose of Ramachandran, by contrast, to generate new passwords that are associated with a particular credit/debit card. If the Ramachandran device permitted passwords to be generated/created, the device would be rendered virtually useless unless the "bank ATM," for instance, was notified what the newly generated PIN is, and the new PIN was also encoded onto the magnetic stripe of the corresponding credit/debit card. Ramachandran provides no structure, nor is any structure even contemplated or suggested due to its futility in conjunction with the Ramachandran device, for generating/creating passwords that can be uniquely associated with a particular secured location. Furthermore, because it would frustrate the purpose of Ramachandran, it is illogical and improper to import such a structural limitation into Ramachandran from another source, i.e., using Ramachandran as the primary or secondary reference in an obviousness type rejection. See, MPEP §2143.01 ("If the proposed modification or combination of the prior art would change the principle or operation of the prior art invention being modified, then the teachings

of the references are not sufficient to render the claims prima facie obvious."), citing In re Ratti, 270 F.2d 810 (CCPA 1959).

The present amendment has cancelled the original claims and presented new claims all of which contain the structure for generating/creating new passwords incorporated into the device. Claim 33 contains the limitation "password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia"; claim 45 contains the structural limitation "password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia"; and claim 53 contains the method step of "instructing said device to randomly generate a string of ascii characters of predetermined length that is representative of a password in response to a prompt generated by said device, wherein said password is uniquely associated with said indicia entered in step b." Each of these three independent claims, the only independent claims in the application as amended, contains the requirement (structural or methodological) for "generating" passwords.

Although the Examiner did comment upon the meaning of the word "generate" in his Action, see page 6 thereof, he also alluded to the fact that Ramachandran does not contain any circuitry for actually creating passwords. Instead, the Examiner understood the term "generate" to be synonomous with "recall." As Ramachandran certainly contains structure for "recalling" passwords stored in its memory, it does not contain circuitry for creating a password. The act of generating/creating, i.e.,

"bringing into being" as phrased by the Examiner, is absent from Ramachandran because the passwords are already created. In fact, if they were not already created and encoded on the magnetic stripe of the individual cards whose data is being transferred to the stand-alone "smart" credit card, the device would be inoperable. Ramachandran only teaches the transferring of a pre-existing password from one location, i.e., a traditional credit/debit card, to another, i.e., a "smart" credit/debit card.

As each of the independent claims added to the present application contain structural limitations not present in, or suggested by any of the prior art references, either singly or in combination, each is patentably distinct. The Examiner's reconsideration in view of these amendments and the foregoing remarks in support thereof, is therefore respectfully requested.

Should the Examiner feel that an interview with Applicant's representative would be useful in advancing the prosecution of this application, he is urged to contact the undersigned at 315-471-3151.

Respectfully submitted,

Joseph Grajewski

By: 9/16/02
George R. McGuire,
Reg. No. 36,603

Hancock & Estabrook, LLP
1500 MONY Tower I
P.O. Box 4976
Syracuse, NY 13221-4976
315-471-3151

VERSION TO SHOW CHANGES MADE

Please delete claims 1 - 32 and add: --

33. A device for use by an authorized individual having a unique biometric parameter to obtain information for use in accessing a secured site, the device comprising:

a. a portable body member;

b. a biometric interface unit engaged with said body member;

c. a non-volatile memory mounted to said body member;

d. biometric circuitry for generating and storing in said non-volatile memory an initialized biometric template upon presentment of the person's unique biometric parameter to said biometric interface unit, and generating a second biometric template upon subsequent presentment of the person's unique biometric parameter to said biometric interface unit;

e. compare circuitry for enabling said device only if said second biometric template is substantially identical to said initialized biometric template;

f. a data storage source;

g. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

h. password circuitry for generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia.

34. The device according to claim 33, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

35. The device according to claim 34, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

36. The device according to claim 35, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

37. The device according to claim 35, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

38. The device according to claim 33, wherein said password circuitry comprises a random number generator.

39. The device according to claim 33, wherein said biometric interface unit is a fingerprint reader.

40. The device according to claim 33, wherein said user interface and communications componentry comprises means for communicating a

preselected string of predetermined length of characters in said data storage source.

41. The device according to claim 40, wherein said means for communicating a preselected string of predetermined length of characters in said data storage source comprises a plurality of arrow keys mounted to said portable body member which may be manipulated and actuated by said individual and which electronically communicate with said device upon actuation by said individual.

42. The device according to claim 33, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

43. The device according to claim 42, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message requiring said individual to reply in order to continue using said device.

44. The device according to claim 43, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

45. A device for use by an authorized individual to obtain information for use in accessing a secured site, the device comprising:

    a. a portable body member;

    b. a data storage source contained in said body member;

c. user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site; and

d. password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia.

46. The device according to claim 45, further comprising indicia selection circuitry for permitting said individual to use said user interface and communications componentry to select one of said plurality of indicia when said device is enabled.

47. The device according to claim 46, further comprising recall circuitry for recalling from said data storage source the one of said passwords that corresponds with said selected one of said plurality of indicia.

48. The device according to claim 47, further comprising output circuitry and a display mounted to said body member for visually displaying said password associated with said selected indicia.

49. The device according to claim 47, further comprising an output communications port connected to said output circuitry for directly transmitting said password corresponding to said selected indicia to said secured site.

50. The device according to claim 45, further comprising means for prompting said individual to change a password corresponding to a predetermined indicia after expiration of a predetermined period of time.

51. The device according to claim 50, wherein said means for prompting said individual to change a password after expiration of a predetermined period of time comprises a clock and circuitry coupled thereto which actuates said device to display a predetermined message requiring said individual to reply in order to continue using said device.

52. The device according to claim 51, wherein said password circuitry will generate a new password and associate said new password with the corresponding one of said indicia for which said prompt was actuated.

53. A method for creating, storing, and managing a password, comprising the steps of:

    a. providing a device comprising a portable body member, a data storage source contained in said body member, user interface and communication componentry for permitting said individual to store in said data storage source a plurality of indicia each one of which is representative of a secured site, and password circuitry comprising a random number generator for randomly generating a plurality of passwords, wherein each of said plurality of passwords is uniquely associated with a respective one of said plurality of indicia;

    b. entering preselected indicia representative of a secured site into said device in response to a prompt generated by said device;

c. instructing said device to randomly generate a string of characters of predetermined length that is representative of a password in response to a prompt generated by said device, wherein said password is uniquely associated with said indicia entered in step b; and

d. repeating steps b and c in sequence for as many times as desired.

54. The method of claim 53, further comprising the step of instructing said device to generate a replacement password for said password created in step c in response to a prompt displayed on said portable body member after a predetermined period of time since said password was created in step c. --

I hereby certify that this correspondence is being placed with the U.S. Postal Service as First Class Mail on this September 16, 2002 addressed to Assistant Commissioner for Patents, Washington D.C. 20231

Ann R. Miller

Dated: 9/16/02